



ZARZĄDZENIE NR 2/2026

**Dyrektora Poznańskiego Ośrodka Specjalistycznych Usług Medycznych
z dnia 22.01.2026 r.**

**w sprawie aktualizacji wewnętrznej procedury dokonywania zgłoszeń
naruszeń prawa i podejmowania działań następczych w Poznańskim Ośrodku
Specjalistycznych Usług Medycznych**

§ 1

Traci moc zarządzenie nr 5/2025 Dyrektora Poznańskiego Ośrodka Specjalistycznych Usług Medycznych z dnia 04.02.2025 r.

§ 2

Ustala się wewnętrzną procedurę dokonywania zgłoszeń naruszeń prawa i podejmowania działań następczych w Poznańskim Ośrodku Specjalistycznych Usług Medycznych, stanowiącą załącznik nr 1 do zarządzenia.

§ 3

Zarządzenie wchodzi w życie z dniem ogłoszenia.

WEWNĘTRZNA PROCEDURA ZGŁOSZEŃ NARUSZEŃ PRAWA I PODEJMOWANIA DZIAŁAŃ NASTĘPCZYCH OBOWIĄZUJĄCA W POZNAŃSKIM OŚRODKU SPECJALISTYCZNYCH USŁUG MEDYCZNYCH

Wersja dokumentu: 3.0

Data zatwierdzenia dokumentu: 19.01.2026

§1 POSTANOWIENIA OGÓLNE

1. Niniejszym wprowadza się wewnętrzną procedurę zgłoszeń naruszeń prawa i podejmowania działań następczych dla sygnalistów („Procedura”) w Poznańskim Ośrodku Specjalistycznych Usług Medycznych, z siedzibą w Poznaniu (61-696), Al. Solidarności 36 (w skrócie: „POSUM”).
2. Celem Procedury jest:
 - a) ograniczenie ryzyka wystąpienia naruszeń,
 - b) wprowadzenie jednolitych wewnętrznych zasad zgłaszania naruszeń dla sygnalistów (bezpiecznych kanałów zgłoszeń), rozpatrywania zgłoszeń w sposób rzetelny i bezstronny oraz podejmowania działań następczych,
 - c) wskazanie wewnętrznych i zewnętrznych warunków objęcia ochroną sygnalistów,
 - d) zapewnienie stosownych środków ochronnych dla sygnalistów, w tym przed działaniami odwetowymi ze strony POSUM lub współpracowników POSUM, w szczególności przeciwko mobbingowi i dyskryminacji,
 - e) zapewnienie odpowiedniego poziomu poufności danych osobowych sygnalisty,
 - f) Niniejsza procedura jest jawna poprzez udostępnienie treści dokumentu na stronie internetowej <https://POSUM.pl/> oraz w BIP: <https://bip.poznan.pl/bip/poznanski-osrodek-specjalistycznych-uslug-medycznych/>.
3. POSUM zobowiązuje się do zapewnienia:
 - a) rzetelnego i niezależnego rozpoznania zgłoszonego naruszenia,

- b) ochrony praw sygnalistów poprzez zapewnienie poufności, w szczególności w zakresie procesu informowania o naruszeniach, rozpatrywania zgłoszeń i podejmowania działań następczych.
4. Procedura została utworzona w związku z dążeniami POSUM do spełnienia wymagań zawartych w:
- a) Dyrektywie Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii (Dz. U. UE. L. z 2019 r. Nr 305, str. 17 z późn. zm.; „Dyrektywa”),
 - b) Przepisach prawa krajowego, w tym implementujących Dyrektywę tj. Ustawie z dnia 14 czerwca 2024 r. o ochronie sygnalistów (Dz. U. poz. 928, ze zm.).

§2 DEFINICJE UŻYTE W PROCEDURZE

1. Przez użyte w Procedurze określenia należy rozumieć:
- a) **sygnalista** – należy przez to rozumieć osobę fizyczną, która zgłasza lub ujawnia publicznie informację o naruszeniu prawa uzyskaną w kontekście związanym z pracą,
 - b) **osoba, której dotyczy zgłoszenie** – należy przez to rozumieć osobę fizyczną, osobę prawną lub jednostkę organizacyjną nieposiadającą osobowości prawnej, której ustawa przyznaje zdolność prawną, wskazaną w zgłoszeniu jako osoba, która dopuściła się naruszenia prawa lub jako osoba, z którą osoba, która dopuściła się naruszenia prawa, jest powiązana,
 - c) **osoba pomagająca w dokonaniu zgłoszenia** – należy przez to rozumieć osobę fizyczną, która pomaga sygnaliście w zgłoszeniu w kontekście związanym z pracą i której pomoc nie powinna zostać ujawniona,
 - d) **osoba powiązana ze sygnalistą** – należy przez to rozumieć osobę fizyczną, która może doświadczyć działań odwetowych w kontekście związanym z pracą, w tym współpracownika lub osobę najbliższą sygnalisty w rozumieniu art. 115 par. 11 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 2024 r., poz. 17 ze zm.) ,
 - e) **procedura** – niniejszy dokument – wewnętrzna procedura zgłaszania informacji o naruszeniach prawa i podejmowania działań następczych,
 - f) **informacja o naruszeniu prawa** – należy przez to rozumieć informację, w tym uzasadnione podejrzenie, dotyczące zaistniałego lub potencjalnego naruszenia prawa, do

którego doszło lub prawdopodobnie dojdzie w POSUM, w którym sygnalista uczestniczył w procesie rekrutacji lub innych negocjacji poprzedzających zawarcie umowy, pracuje lub pracował, lub w innym podmiocie prawnym, z którym sygnalista utrzymuje lub utrzymywał kontakt w kontekście związanym z pracą, lub informację dotyczącą próby ukrycia takiego naruszenia prawa,

g) **informacja zwrotna** – należy przez to rozumieć przekazanie sygnaliście informacji na temat planowanych lub podjętych działań następczych i powodów takich działań,

h) **kontekst związany z pracą** – należy przez to rozumieć przeszłe, obecne lub przyszłe działania związane z wykonywaniem pracy na podstawie stosunku pracy lub innego stosunku prawnego stanowiącego podstawę świadczenia pracy lub usług lub pełnienia funkcji w POSUM lub na rzecz POSUM, w ramach których uzyskano informację o naruszeniu prawa oraz istnieje możliwość doświadczenia działań odwetowych,

i) **naruszenie** – sytuacja nieprawidłowa, stanowiąca naruszenie prawa i wymagająca zgłoszenia Koordynatorowi ds. Zgłoszeń, która jest uzasadniona i wynika z wiedzy zdobytej przez sygnalistę,

j) **działanie następcze lub postępowanie wyjaśniające** – należy przez to rozumieć działanie podjęte przez POSUM w celu oceny prawdziwości informacji zawartych w zgłoszeniu w tym określonych w Procedurze oraz, w stosownych przypadkach, w celu przeciwdziałania naruszeniu prawa będącemu przedmiotem zgłoszenia, w szczególności przez postępowanie wyjaśniające, wszczęcie kontroli lub postępowania administracyjnego, wniesienie oskarżenia, działanie podjęte w celu odzyskania środków finansowych lub zamknięcie procedury realizowanej w ramach wewnętrznej procedury zgłaszania naruszeń prawa i nie podejmowania działań następczych,

k) **działanie odwetowe** – należy przez to rozumieć bezpośrednie lub pośrednie działanie lub zaniechanie w kontekście związanym z pracą, które jest spowodowane zgłoszeniem, i które narusza lub może naruszyć prawa sygnalisty lub wyrządza lub może wyrządzić nieuzasadnioną szkodę sygnaliście, w tym niezasadne wszczynanie postępowań przeciwko sygnaliście,

l) **organ publiczny** – należy przez to rozumieć naczelne i centralne organy administracji rządowej, terenowe organy administracji rządowej, organy jednostek samorządu terytorialnego, inne organy państwowe oraz inne podmioty wykonujące z mocy prawa zadania z zakresu administracji publicznej właściwe do podejmowania działań następczych w zakresie swojego działania,

m) **rejestr** – oznacza to Rejestr zgłoszonych naruszeń,

- n) **zgłoszenie** – należy przez to rozumieć ustne lub pisemne, dokonane w postaci papierowej lub elektronicznej, zgłoszenie wewnętrzne lub zewnętrzne, przekazane zgodnie z wymogami określonymi w Procedurze i obowiązujących przepisach prawa,
- o) **zgłoszenie wewnętrzne** – należy przez to rozumieć zgłoszenie o naruszeniu prawa przekazane POSUM zgodnie z wymogami określonymi w Procedurze,
- p) **Koordinator ds. Zgłoszeń** – należy przez to rozumieć osobę wyznaczoną do przyjmowania zgłoszeń naruszeń w ramach Procedury, wstępnej weryfikacji i komunikacji z zgłaszającym, to jest: doradcy podmiot zewnętrzny, na podstawie odrębnej umowy.
- r) **Komisja Wyjaśniająca (Komisja)** – należy przez to rozumieć wewnętrzny zespół osób, powołanych przez Dyrektora POSUM do weryfikacji zgłoszeń; podjęcia działań następczych i występowania o dodatkowe informacje i dokumenty.

§ 3 ZAKRES ZASTOSOWANIA PROCEDURY

1. Naruszeniem prawa jest działanie lub zaniechanie niezgodne z prawem, zasadami obowiązującymi w POSUM lub mające na celu obejście prawa dotyczące:
 - a) korupcji,
 - b) zamówień publicznych,
 - c) usług, produktów i rynków finansowych,
 - d) przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu,
 - e) bezpieczeństwa produktów i ich zgodności z wymogami,
 - f) bezpieczeństwa transportu,
 - g) ochrony środowiska,
 - h) ochrony radiologicznej i bezpieczeństwa jądrowego,
 - i) zdrowia publicznego,
 - j) ochrony konsumentów,
 - k) ochrony prywatności i danych osobowych,
 - l) bezpieczeństwa sieci i systemów teleinformatycznych,

- m) interesów finansowych Skarbu Państwa Rzeczypospolitej Polskiej, jednostki samorządu terytorialnego oraz Unii Europejskiej,
- n) konstytucyjnych wolności i praw człowieka i obywatela – występujące w stosunkach jednostki z organami władzy publicznej i niezwiązane z dziedzinami wskazanymi w powyżej w pkt a) – m).
2. Procedura nie uwzględnia możliwości dokonywania zgłoszeń innych niż wskazanych powyżej naruszeń. W przypadku wystąpienia takich naruszeń, zgłoszenia należy dokonać w normalnym toku wykonywania obowiązków.
 3. Zgłoszenie naruszenia może być dokonane wyłącznie w dobrej wierze.
 4. Zakazuje się świadomego składania fałszywych zgłoszeń naruszenia.
 5. W przypadku ustalenia w wyniku wstępnej analizy zgłoszenia albo w toku postępowania wyjaśniającego, iż w zgłoszeniu naruszenia świadomie podano nieprawdę lub zatajono prawdę, zgłaszający będący Pracownikiem, może zostać pociągnięty do odpowiedzialności porządkowej określonej w przepisach Kodeksu Pracy. Zachowanie takie może być również zakwalifikowane jako ciężkie naruszenie podstawowych obowiązków pracowniczych i jako takie skutkować rozwiązaniem umowy o pracę bez zachowania okresu wypowiedzenia.
 6. W przypadku zgłaszającego, świadczącego na rzecz POSUM usługi lub dostarczającego towary na podstawie umowy cywilnoprawnej, ustalenie dokonania fałszywego zgłoszenia naruszenia skutkować może rozwiązaniem umowy lub definitywnym zakończeniem współpracy pomiędzy stronami, grzywną, karą ograniczenia lub pozbawienia wolności do lat 2.
 7. Niezależnie od skutków wskazanych powyżej, zgłaszający, świadomie dokonujący fałszywego zgłoszenia naruszenia może zostać pociągnięty do odpowiedzialności odszkodowawczej w przypadku wystąpienia szkody w związku z fałszywym zgłoszeniem.
 8. Procedura zgłoszeń wewnętrznych nie ma zastosowania dla **zgłoszeń anonimowych**. Zgłoszenia anonimowe nie będą przyjmowane i pozostaną zostawione bez rozpoznania.

§ 4 SYGNALISTA

1. Sygnalistą, w rozumieniu niniejszej Procedury, może być:
 - b) pracownik,
 - c) pracownik tymczasowy,
 - d) osoba świadcząca pracę na innej podstawie niż stosunek pracy, w tym na podstawie umowy cywilnoprawnej,
 - e) przedsiębiorca,
 - f) prokurent,
 - g) osoba świadcząca pracę pod nadzorem i kierownictwem wykonawcy, podwykonawcy lub dostawcy POSUM, w tym na podstawie umowy cywilnoprawnej,
 - h) stażysta,
 - i) wolontariusz,
 - j) praktykant,
2. Procedurę stosuje się także do osoby fizycznej, o której mowa w pkt 1, w przypadku zgłoszenia informacji o naruszeniu prawa uzyskanej w kontekście związanym z pracą przed nawiązaniem stosunku pracy lub innego stosunku prawnego stanowiącego podstawę świadczenia pracy lub usług na rzecz POSUM lub gdy taki stosunek już ustał.
3. Sygnalista podlega ochronie określonej w Procedurze i obowiązujących przepisach prawa krajowego, od chwili dokonania zgłoszenia pod warunkiem, że miał uzasadnione podstawy sądzić, że będąca przedmiotem zgłoszenia informacja jest prawdziwa w momencie dokonywania zgłoszenia i że informacja taka stanowi informację o naruszeniu prawa.
4. Dane osobowe sygnalisty pozwalające na ustalenie jego tożsamości oraz inne informacje, na podstawie których można bezpośrednio lub pośrednio zidentyfikować tożsamość sygnalisty nie podlegają ujawnieniu nieupoważnionym osobom, chyba że za wyraźną zgodą sygnalisty.
5. Postanowienie punktu 4 powyżej nie znajduje zastosowania w przypadku, w którym ujawnienie jest koniecznym i proporcjonalnym obowiązkiem wynikającym z przepisów prawa w związku z postępowaniami wyjaśniającymi prowadzonymi przez organy publiczne lub postępowaniami przygotowawczymi lub sądowymi prowadzonymi przez

sądy, w tym w celu zagwarantowania prawa do obrony przysługującego osobie, której dotyczy zgłoszenie.

6. POSUM po otrzymaniu zgłoszenia przetwarza dane osobowe w zakresie niezbędnym do przyjęcia zgłoszenia lub podjęcia ewentualnego działania następczego. Dane osobowe, które nie mają znaczenia dla rozpatrywania zgłoszenia, nie są zbierane, a w razie przypadkowego zebrania są niezwłocznie usuwane. Usunięcie tych danych osobowych następuje w terminie 14 dni od chwili ustalenia, że nie mają one znaczenia dla sprawy.

§ 5 SPOSOBY DOKONYWANIA ZGŁOSZEŃ

1. Sygnalista może dokonać zgłoszenia wewnętrznego w formie pisemnej:
 - a) elektronicznie – imiennie:
 - za pośrednictwem strony internetowej POSUM, w zakładce - SYGNALIŚCI: <https://posum.pl/sygnaliści>, pod przyciskiem „Zgłoszenie naruszenia”,
 - bezpośrednio na adres poczty elektronicznej: zgloszenie.wewnetrzne@posum.pl
 - b) listownie – imiennie, pocztą tradycyjną na adres korespondencyjny: Al. Solidarności 36, Poznań, Sekretariat Dyrektora POSUM. W celu zachowania pełnej poufności korespondencji oraz danych sygnalisty, prosimy na kopercie dopisać „**zgłoszenie wewnętrzne**”. Na kopercie nie należy podawać żadnych danych osobowych nadawcy, a przesyłka pocztowa powinna zostać nadana w formie listu zwykłego.
2. Pracownicy punktu kancelaryjnego obsługującego przesyłki pocztowe, o których mowa w ust. 1b:
 - a) nie otwierają i nie odwzorowują cyfrowo koperty i zawartości przesyłki pocztowej,
 - b) umieszczają na kopercie pieczęć wpływu i dokonują rejestracji przesyłki pocztowej w rejestrze przesyłek przychodzących wpisując nazwę „zgłoszenie wewnętrzne”, bez rejestracji danych osobowych,
 - c) przekazują przesyłkę pocztową w stanie nienaruszonym bezpośrednio do Koordynatora ds. Zgłoszeń.
3. Jeżeli przesyłka pocztowa ze zgłoszeniem wewnętrznym pisemnym została skierowana przez nadawcę, pod inny adres niż wskazany w ust. 1b lub do innej komórki organizacyjnej POSUM, stosuje się odpowiednio ust. 2.

4. Jeżeli przesyłka pocztowa ze zgłoszeniem wewnętrznym pisemnym nie zawiera na kopercie dopisku, o którym mowa w ust. 1b, co skutkuje jej otwarciem, stosuje się odpowiednio ust. 2.
5. Kanały zgłoszeniowe są bezpieczne i zapewniają poufność danych. Dostęp do kanałów zgłoszeniowych posiada tylko Koordynator ds. Zgłoszeń.
6. Procedura nie uwzględnia innych możliwości dokonywania zgłoszeń, tzn. w innej formie, ani zgłoszeń anonimowych.
7. Zgłoszenia należy dokonywać w języku polskim.
8. Zgłaszający, dokonując zgłoszenia może skorzystać ze wzoru zgłoszenia naruszenia, stanowiącego Załącznik nr 1 do Procedury.
9. W celu rzetelnej weryfikacji zgłoszenia oraz skutecznego podjęcia działania następczych zaleca się, aby zgłoszenie zawierało wszelkie dane, o których mowa we wzorze zgłoszenia naruszenia (Załącznik nr 1 do Procedury) w szczególności :
 - a) dane osobowe sygnalisty oraz osoby której dotyczy zgłoszenie,
 - b) adres do kontaktu sygnalisty,
 - c) datę oraz miejsce zaistnienia naruszenia
 - d) możliwie dokładny opis przedmiotu naruszenia (stan faktyczny, który budzi wątpliwości sygnalisty)
 - e) wskazanie podmiotu, którego dotyczy zgłoszenie naruszenie,
 - f) wskazanie ewentualnych świadków naruszenia,
 - g) wskazanie wszystkich dowodów i informacji, jakimi dysponuje zgłaszający, które mogą okazać się pomocne w procesie rozpatrywania naruszenia.
 - h) opis kontekstu związanego z pracą, który umożliwił dostrzeżenie zgłoszonego naruszenia,
 - i) wskazanie uzasadnionych podstaw, które umożliwiły stwierdzenie, że informacja o naruszeniu prawa jest prawdziwa.
10. Zgłaszający zobowiązany jest do traktowania posiadanych przez niego informacji dotyczących podejrzenia naruszenia jako tajemnicy i powstrzymania się od publicznych rozmów o zgłaszanych podejrzeniach naruszenia, chyba że osoba ta jest zobowiązana do takiego działania przepisami prawa.

11. Sygnalista, dokonując zgłoszenia wewnętrznego pisemnego na adres poczty elektronicznej: zgloszenie.wewnetrzne@posum.pl powinien zaszyfrować zawartość przesyłki.
12. W przypadku szyfrowania przesyłki, treść zgłoszenia wewnętrznego pisemnego nie powinna być umieszczona bezpośrednio w wiadomości elektronicznej, lecz w załączonym do tej wiadomości zaszyfrowanym pliku.
13. Pomocnicza instrukcja szyfrowania zawartości przesyłki ze zgłoszeniem wewnętrznym pisemnym, dokonywanym na adres, o którym mowa w ust. 1a, stanowi załącznik do procedury zgłoszeń wewnętrznych.
14. Dokonując zgłoszenia wewnętrznego pisemnego, o którym mowa w ustępach poprzedzających, Sygnalista przekazuje upoważnionej osobie hasło do otwarcia zaszyfrowanej zawartości przesyłki inną drogą, niż na adres poczty elektronicznej, o którym mowa w ust. 1a w sposób, uzgodniony z upoważnioną osobą pod numerem telefonu **+48 534 270 703** .

§ 6 OSOBY UPOWAŻNIONE - KOORDYNATOR DS. ZGŁOSZEŃ, KOMISJA WYJAŚNIAJĄCA

1. Koordynatorem ds. Zgłoszeń, upoważnionym przez Dyrektora POSUM do przyjmowania zgłoszeń wewnętrznych jest podmiot zewnętrzny: Kancelaria Bezpieczeństwa Informacji sp. z o.o. k. (ul. Święty Marcin 29/8, 61-806 Poznań). Podmiot upoważniony otrzymuje zgłoszenia dokonane w formie elektronicznej, a także korespondencję kierowaną na adres stacjonarny (listowną).
2. Jeżeli zgłoszenie zostało dokonane inaczej niż w sposób, określony w ust. 1 niniejszego paragrafu i odbiorcą zgłoszenia nie jest Koordynator ds. Zgłoszeń, zgłoszenia takie należy niezwłocznie do niego przekazać. Nieprzekazywanie informacji i zgłoszeń do osoby upoważnionej lub blokowanie ich obiegu stanowi ciężkie naruszenie obowiązków pracowniczych albo poważne naruszenie umowy zawartej z POSUM i stanowi podstawę do rozwiązania umowy o pracę bez wypowiedzenia z winy pracownika, albo ważny powód będący podstawą wypowiedzenia lub odstąpienia od innej umowy ze skutkiem natychmiastowym.
3. Koordynator ds. Zgłoszeń jest odpowiedzialny w szczególności za:
 - a) przyjmowanie zgłoszeń wewnętrznych
 - b) wstępną weryfikację zgłoszenia,

- c) prowadzenia rejestru zgłoszeń naruszeń prawa od sygnalistów,
 - d) prowadzenie korespondencji z sygnalistą, w tym: przekazanie informacji zwrotnej, występowania o dodatkowe informacje,
 - e) informowanie sygnalistów o podjętych działaniach następczych, wynikających z otrzymania informacji o naruszeniach prawa,
 - f) prowadzenia i przechowywania akt spraw dotyczących zgłoszeń naruszeń prawa od sygnalistów.
4. Do podejmowania działań następczych upoważniona jest Komisja Wyjaśniająca.
 5. Komisja Wyjaśniająca jest powoływana przez Dyrektora POSUM. Komisja składa się z 2 do 5 członków. W skład Komisji wchodzi pracownicy POSUM, posiadający wiedzę, doświadczenie i umiejętności przydatne przy rozpatrywaniu danego zgłoszenia. Członkami Komisji, w razie potrzeby, mogą być również zewnętrzne podmioty doradcze, na podstawie odrębnej umowy.
 6. Członkiem Komisji Wyjaśniającej nie może być osoba, której dotyczy zgłoszenie.
 7. Komisja Wyjaśniająca jest obowiązana do:
 - a) weryfikacji zgłoszeń,
 - b) prowadzenie postępowań wyjaśniających zgłoszenia, w tym występowania o dodatkowe informacje,
 - c) podejmowanie bądź inicjowanie i nadzór nad działaniami następczymi w ramach wewnętrznej struktury POSUM,
 - d) monitorowanie sytuacji sygnalisty, w celu zapewnienia właściwej ochrony sygnaliście w ramach jego funkcjonowania lub współpracy z POSUM.
 8. POSUM gwarantuje, że Procedura oraz związane z przyjmowaniem zgłoszeń przetwarzanie danych osobowych uniemożliwiają nieupoważnionym osobom uzyskanie dostępu do informacji objętych zgłoszeniem oraz zapewniają ochronę poufności tożsamości sygnalisty, osoby, której dotyczy zgłoszenie, oraz osoby trzeciej wskazanej w zgłoszeniu. Ochrona poufności dotyczy informacji, na podstawie których można bezpośrednio lub pośrednio zidentyfikować tożsamość sygnalisty lub takich osób.
 9. Do przyjmowania i weryfikacji zgłoszeń wewnętrznych, podejmowania działań następczych oraz przetwarzania danych osobowych, mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie nadane przez Dyrektora POSUM. Osoby upoważnione są obowiązane do zachowania tajemnicy w zakresie informacji i danych

osobowych, które uzyskały w ramach przyjmowania i weryfikacji zgłoszeń wewnętrznych, oraz podejmowanych działań następczych, także po ustaniu stosunku pracy lub innego stosunku prawnego, w ramach którego wykonywały tę pracę.

§ 7. ROZPATRYWANIE ZGŁOSZENIA, INFORMACJE ZWROTNE, DZIAŁANIA NASTĘPCZE

1. Po wpływie zgłoszenia jest ono rozpatrywane zgodnie z zasadami określonymi w Procedurze, o ile charakter i przedmiot zgłoszenia nie uzasadniają rozpatrzenia go w trybie przewidzianym odrębnymi regulacjami bądź przepisami prawa powszechnie obowiązującego.
2. Po otrzymaniu zgłoszenia wewnętrzne Koordynator ds. Zgłoszenia obowiązany jest:
 - a) dokonać wstępnej analizy zgłoszenia
 - b) niezwłocznie zarejestrować zgłoszenie w rejestrze zgłoszeń,
 - c) niezwłocznie po zarejestrowaniu, nie później niż w ciągu 7 dni od daty przyjęcia zgłoszenia przekazać sygnaliście potwierdzenie przyjęcia zgłoszenia,
3. Informacja zwrotna obejmuje w szczególności informacje na temat planowanych lub podjętych działań następczych oraz rekomendacjach, których celem jest wyeliminowanie i zapobieganie tożsamym lub podobnym naruszeniom co opisane w zgłoszeniu i powodów takich działań.
4. Koordynator ds. Zgłoszeń dokonuje wstępnej analizy zgłoszenia pod kątem tego, czy informacje w nim zawarte umożliwiają rozpatrzenie zasadności zgłoszenia, a gdy zajdzie taka potrzeba, kontaktuje się ze sygnalistą, o udzielenie wyjaśnień lub dodatkowych informacji dotyczących zgłoszenia wewnętrznego.
5. Komisja Wyjaśniająca może podjąć decyzję o odstąpieniu od przeprowadzenia postępowania wyjaśniającego w przypadku, gdy:
 - a) zdarzenie opisowe nie miało miejsca,
 - b) zgłoszenie wewnętrzne zostało dokonane w złej wierze,
 - c) naruszenie nie mieści się w zakresie obszarów naruszeń wskazanych w Procedurze,
 - d) zgłoszenie jest w oczywisty sposób niewiarygodne lub bezzasadne,
 - e) niemożliwe jest uzyskanie informacji niezbędnych do prowadzenia postępowania

wyjaśniającego i podjęcia działań następczych.

6. Jeśli zgłoszenie pozwala na przeprowadzenie weryfikacji jego zasadności, a ponadto według opisu zgłoszenia zachodzi prawdopodobieństwo wystąpienia naruszeń, następuje wszczęcie postępowania wyjaśniającego w ramach Komisji.
7. Komisja może zaangażować w postępowanie wyjaśniające i dotyczące podjęcia działań następczych przedstawicieli innych komórek organizacyjnych POSUM lub niezależnego konsultanta, których wiedza i doświadczenie mogą być niezbędne w przepracowaniu zgłoszenia.
8. Komisja rozpatruje zgłoszenie, podejmuje działania następcze oraz przekazuje do Koordynatora ds. zgłoszeń informacje zwrotne bez zbędnej zwłoki, nie później jednak niż w terminie 3 miesięcy od dnia potwierdzenia przyjęcia zgłoszenia.
9. Za działania następcze uznaje się czynności:
 - a) weryfikacja informacji o naruszeniu i ocena prawidłowości zarzutów,
 - b) przeprowadzenie postępowania wyjaśniającego,
 - c) wysłuchanie sygnalisty,
 - d) usunięcie naruszenia,
 - e) podjęcie środków zapobiegawczych celem niewystępowania nieprawidłowości,
 - f) zamknięcie procedury działań następczych.
10. Komisja, może podejmować działania w celu zweryfikowania informacji o naruszeniu takich jak m.in. odbieranie wyjaśnień w celu zgromadzenia dodatkowych informacji oraz uzyskanie kopii dokumentów.
11. Komisja ma obowiązek podejmowania czynności, z zachowaniem należytej staranności i poufności, w sposób uczciwy i bezstronny.
12. W przypadku, gdy zajdzie taka konieczność, Komisja może wezwać na posiedzenie pracowników lub współpracowników, którzy mogą mieć związek lub jakąkolwiek wiedzę w zakresie zgłoszenia wewnętrznego, lub sygnalisty, w celu złożenia wyjaśnień. Na wniosek Komisji prowadzącej postępowanie wyjaśniające, wszyscy pracownicy mają obowiązek stawić się na posiedzeniu oraz zobowiązani są do współpracy w ramach postępowania wyjaśniającego i podejmowania działań następczych, w szczególności udzielania zgodnych z prawdą informacji lub wyjaśnień oraz przedstawiania kompletnych dokumentów.

13. Wyjaśnienia składane przez wezwane osoby utrwalane są w formie protokołu.
14. Po ustaleniu całokształtu stanu faktycznego Komisja podejmuje decyzję co do zasadności zgłoszenia, a w przypadku zgłoszeń zasadnych również wydaje rekomendacje o stosownych działaniach naprawczych lub dyscyplinujących w stosunku do pracownika lub współpracownika, który dopuścił się naruszenia, oraz rekomendację możliwych działań zapobiegawczych mających na celu wyeliminowanie podobnych do opisanych w zgłoszeniu wewnętrznych naruszeń w przyszłości.
15. Wnioski końcowe zawierają w szczególności: wskazanie osób wchodzących w skład Komisji, datę otrzymania zgłoszenia wewnętrznego, opis stanu faktycznego, opisu podjętych czynności, opis zebranych dowodów, rodzaj naruszenia, decyzję w przedmiocie zasadności zgłoszenia oraz – w sytuacji zgłoszeń uznanych za zasadne – rekomendację stosownych działań następczych i zapobiegawczych.
16. Rekomendacje, mogą obejmować w szczególności: zamknięcie postępowania bez podejmowania dalszych działań; przeprowadzenie rozmowy z osobą, której zgłoszenie dotyczy; upomnienie, nałożenie kary finansowej; wnioski prewencyjne (zalecenia, procedury) o charakterze zarządczym; zmiany w wewnętrznej organizacji POSUM, podjęcie działań cywilno-prawnych np. naprawienie szkody, odszkodowanie; wszczęcie postępowania dyscyplinarnego, złożenie zawiadomienia o uzasadnionym podejrzeniu przestępstwa; poinformowanie właściwych służb /organów/instytucji.
17. Ustalenia, wnioski i rekomendacje, o których mowa w pkt 14,15,16 powyżej są utrwalane w formie protokołu.
18. W przypadku pozytywnej weryfikacji zasadności zgłoszenia Komisja:
 - a) przekazuje informację o wyniku postępowania wyjaśniającego do Dyrektora POSUM, w celu podjęcia stosownych, następczych działań dyscyplinujących lub naprawczych zawartych w protokole wobec osoby, której zarzuca się dokonanie naruszenia,
 - b) w terminie do 7 dni roboczych od przekazania informacji, o której mowa w pkt a) powyżej, informuje osobę, której zarzuca się dokonanie naruszenia, o dokonanym zgłoszeniu oraz przeprowadzonej weryfikacji zgłoszenia wewnętrznego.
19. W przypadku negatywnej weryfikacji zasadności zgłoszenia wewnętrznego i oddalenia podejrzeń w nim zawartych Komisja, przekazuje niezwłocznie sygnaliście oraz osobie, której zarzucano dokonanie naruszenia, informację o dokonanym zgłoszeniu

- wewnętrznym oraz o przeprowadzonej weryfikacji zgłoszenia wewnętrznego i jej wyniku.
20. Informacje, o których mowa w pkt 18 i 19, przekazywane są sygnaliście, w nieprzekraczalnym 3-miesięcznym terminie od potwierdzenia przyjęcia zgłoszenia wewnętrznego.
 21. Osoba dokonująca zgłoszenia imiennie, w dobrej wierze, ma prawo do uzyskania statusu sygnalisty w zakresie: zachowania w poufności jego danych osobowych (dostęp do danych osobowych posiadają wyłącznie osoby upoważnione, z zastrzeżeniem sytuacji, gdy osoba zgłaszająca wyrazi zgodę na ujawnienie swoich danych osobowych lub ujawnienie tych danych jest koniecznym i proporcjonalnym obowiązkiem wynikającym z powszechnie obowiązującego prawa w kontekście prowadzonych przez organy krajowe postępowań. Prawo ochrony przewidzianej w niniejszym punkcie nie przysługuje: osobie dokonującej zgłoszenia w złej wierze lub dokonująca zgłoszenia niepoważnego lub zgłoszenia niestanowiącego w istocie naruszenia.

8 DZIAŁANIA ODWETOWE

1. Wobec sygnalistów, osób pomagających w dokonaniu zgłoszenia lub osób powiązanych z sygnalistą zakazuje się podejmowania działań odwetowych.
2. Koordynator ds. Zgłoszeń oraz członkowie Komisji zobowiązani są podczas postępowania wyjaśniającego do:
 - a) zachowania informacji, w tym danych osobowych pozyskanych w trakcie postępowania wyjaśniającego w tajemnicy wobec osób trzecich;
 - b) traktowania wszystkich osób biorących udział w postępowaniu wyjaśniającym w sposób sprawiedliwy, z poszanowaniem ich godności i dóbr osobistych;
 - c) zachowania neutralności, obiektywizmu podczas prowadzonego postępowania;
 - d) przestrzegania zasad ochrony sygnalisty;
 - e) w trakcie postępowania stosować adekwatne, niezbędne i proporcjonalne środki służące do osiągnięcia celu postępowania.
3. Sygnalista, który doświadczy działań odwetowych w związku ze swoim zgłoszeniem powinien poinformować o tym fakcie Koordynatora ds. Zgłoszeń. Koordynator ds. Zgłoszeń zobowiązany jest do podjęcia działań mających na celu ochronę sygnalisty.

4. Podejmowanie działań odwetowych stanowi ciężkie naruszenie obowiązków pracowniczych, albo poważne naruszenie warunków umowy, które uzasadnia rozwiązanie umowy o pracę bez wypowiedzenia, albo wypowiedzenie lub odstąpienie od innej umowy ze skutkiem natychmiastowym. Niezależnie od powyższego osoba podejmująca działania odwetowe podlega odpowiedzialności karnej - grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2, a jeżeli sprawca działa w sposób uporczywy, podlega karze pozbawienia wolności do lat 3.

§ 9. ZGŁOSZENIA ZEWNĘTRZNE

1. Sygnalista może dokonać zgłoszenia zewnętrznego do Rzecznika Praw Obywatelskich lub organu publicznego oraz w stosownych przypadkach do instytucji, organów lub jednostek organizacyjnych Unii Europejskiej, w sprawach i na zasadach określonych w ustawie z dnia 14 czerwca 2024 r. o ochronie sygnalistów, bez uprzedniego dokonania zgłoszenia wewnętrznego.
2. Zgłoszenie zewnętrzne może być dokonane ustnie lub pisemnie.
3. Zgłoszenie zewnętrzne w formie dokumentowej może być dokonane:
 - a) w postaci papierowej - na adres do korespondencji wskazany przez Rzecznika Praw Obywatelskich lub organ publiczny przyjmujący zgłoszenie;
 - b) w postaci elektronicznej - na adres poczty elektronicznej lub adres elektronicznej skrzynki podawczej, lub adres do doręczeń elektronicznych, wskazane przez Rzecznika Praw Obywatelskich lub organ publiczny przyjmujący zgłoszenie, lub za pośrednictwem przeznaczonego do tego formularza internetowego lub aplikacji wskazanej przez organ publiczny jako aplikacja właściwa do dokonywania zgłoszeń w postaci elektronicznej.
4. Informacje dla sygnalistów dotyczące zgłoszeń zewnętrznych Rzecznik Praw Obywatelskich oraz organy publiczne umieszczają na swoich stronach w Biuletynie Informacji Publicznej w oddzielnej, łatwo identyfikowalnej i dostępnej sekcji.
5. Jednym z organów publicznych w rozumieniu ustawy jest Prezydent Miasta Poznania. Komórką organizacyjną Urzędu Miasta Poznania, wyznaczoną przez Prezydenta Miasta Poznania do przyjmowania zgłoszeń zewnętrznych i podejmowania działań następczych, włączając w to weryfikację zgłoszeń, dalszą komunikację ze zgłaszającymi, w tym występowanie o dodatkowe informacje i przekazywanie

zgłaszającym informacji zwrotnych, jest Biuro Kontroli Urzędu Miasta Poznania.

6. Zgłoszenie zewnętrzne może być dokonane również do odpowiednich organów i jednostki organizacyjnych Unii, takich jak Europejski Urząd ds. Zwalczenia Nadużyć Finansowych (OLAF), Europejska Agencja Bezpieczeństwa Morskiego (EMSA), Europejska Agencja Bezpieczeństwa Lotniczego (EASA), Europejski Urząd Nadzoru Giełd i Papierów Wartościowych (ESMA) i Europejska Agencja Leków (EMA), które dysponują zewnętrznymi kanałami i procedurami dokonywania zgłoszeń służącymi do przyjmowania zgłoszeń.
7. Zgłoszenie kierowane do instytucji, organów lub jednostek organizacyjnych Unii Europejskiej opisane zostały m.in. na oficjalnych stronach internetowych Unii Europejskiej, takich jak: https://european-union.europa.eu/contact-eu/make-complaint_pl , a w zakresie dotyczącym praw człowieka m.in. na stronie https://commission.europa.eu/aid-development-cooperation-fundamental-rights/your-rights-eu/how-report-breach-your-rights_pl
8. Sprawę naruszeń przepisów unijnych można zgłosić poprzez:
 - a) skargę do Komisji Europejskiej jeśli składający skargę uważa, że kraj Unii Europejskiej naruszył unijne przepisy przyjmując ustawę lub rozporządzenie albo podejmując działania administracyjne,
 - b) skargę do Europejskiego Rzecznika Praw Obywatelskich, jeśli składający skargę uważa, że instytucja, organ albo agencja Unii Europejskiej nie postępuje zgodnie z prawem lub zasadami dobrego administrowania lub narusza prawa człowieka,
 - c) petycję do Parlamentu Europejskiego dotyczącą stosowania prawa Unii Europejskiej,
 - d) zgłoszenie związane z finansowaniem Unii Europejskiej albo pracownikami Unii Europejskiej do Europejskiego Urzędu ds. Zwalczenia Nadużyć Finansowych (OLAF).

§ 10. REJESTR ZGŁOSZONYCH NARUSZEŃ

1. Tworzy się rejestr zgłoszonych naruszeń, zwany Rejestrem. Wzór Rejestru stanowi załącznik nr 3 do niniejszej Procedury.
2. Rejestr jest prowadzony przez Koordynatora ds. Zgłoszeń.
3. Rejestr zawiera:
 - a) numer zgłoszenia;

- b) przedmiot naruszenia prawa;
 - c) dane osobowe sygnalisty oraz osoby, której dotyczy zgłoszenie, niezbędne do identyfikacji tych osób;
 - d) adres do kontaktu sygnalisty;
 - e) datę dokonania zgłoszenia;
 - f) informację o podjętych działaniach następczych;
 - g) datę zakończenia sprawy.
4. Administratorem danych zawartych w Rejestrze jest Poznański Ośrodek Specjalistycznych Usług Medycznych - POSUM.
 5. Rejestr prowadzony jest z zachowaniem zasad poufności, a dokumenty i informacje zebrane w toku analizy oraz informacje dotyczące rozpatrzenia zgłoszenia przechowywane są przez okres 3 lat po zakończeniu roku kalendarzowego, w którym zakończono działania następcze, lub po zakończeniu postępowań zainicjowanych tymi działaniami.
 6. Dostęp do Rejestru przysługuje wyłącznie upoważnionym osobom: Koordynatorowi ds. Zgłoszeń, członkom Komisji. Dostęp do Rejestru przysługuje także organom ścigania w związku z prowadzonymi czynnościami wynikającymi z powszechnie obowiązujących przepisów prawa.

§ 11. POSTANOWIENIA KOŃCOWE

1. Niniejsza Procedura wchodzi w życie po upływie 7 dni od dnia podania jej do wiadomości pracownikom POSUM poprzez umieszczenie jej na stronie internetowej pod adresem: <https://posum.pl/> oraz w Biuletynie Informacji Publicznej (BIP).
2. Informację o Procedurze przekazuje się osobie ubiegającej się o pracę na podstawie stosunku pracy lub innego stosunku prawnego stanowiącego podstawę świadczenia pracy lub usług w POSUM wraz z rozpoczęciem rekrutacji lub negocjacji poprzedzających zawarcie umowy.
3. Dyrektor POSUM informują pracowników POSUM o wejściu w życie Procedury oraz jej zmianach. Kierownicy innych jednostek organizacyjnych POSUM zobowiązani są do zapoznania z Procedurą wszystkich podległych im pracowników.

4. Procedura podlegała uzgodnieniu ze związkami zawodowymi działającymi w POSUM.
5. Za adekwatność i skuteczność funkcjonowania Procedury odpowiedzialne jest Dyrektor POSUM.
6. POSUM, w zależności od potrzeb, nie rzadziej niż raz w roku, ocenia adekwatność i skuteczność funkcjonowania Procedury. Zmian Procedury dokonuje się w tym samym trybie jak jej utworzenie.
7. W sprawach nieuregulowanych niniejszą Procedurą stosuje się odpowiednio przepisy powszechnie obowiązującego prawa w zakresie ochrony sygnalistów.
8. We wszystkich kwestiach dotyczących Procedury osobą dedykowaną do kontaktu jest Koordynator ds. Zgłoszeń dostępny pod numerem: **+48 534 270 703**

WYKAZ ZAŁĄCZNIKÓW

Załącznik nr 1 do Procedury – Wzór zgłoszenia naruszenia wewnętrznego wraz z klauzulą informacyjną w związku z przetwarzaniem danych osobowych sygnalisty

Załącznik nr 2 do Procedury – Wzór potwierdzenia otrzymania zgłoszenia wewnętrznego

Załącznik nr 3 do Procedury – Wzór rejestru zgłoszonych naruszeń

Załącznik nr 4 do Procedury – Wzór oświadczenia o zapoznaniu się z procedurą zgłaszania informacji o naruszeniach prawa i podejmowania działań następczych

Załącznik nr. 5 do Procedury – Wzór klauzuli informacyjnej dla osób wskazanych w zgłoszeniu wewnętrznym

Załącznik nr 6 do Procedury – Wzór upoważnienia do przetwarzania danych osobowych

Załącznik nr 7 do Procedury – Pomocnicza instrukcja szyfrowania zawartości przesyłki (zgłoszenia dokonywane elektronicznie)

.....

(miejscowość, data)

Załącznik nr 1 do Procedury – Wzór zgłoszenia naruszenia wewnętrznego wraz z klauzulą informacyjną w związku z przetwarzaniem danych osobowych sygnalisty

ZGŁOSZENIE NARUSZENIA WEWNĘTRZNEGO

Nr

Formularz służy zgłaszaniu naruszeń w POSUM. Podane informacje są objęte poufnością na zasadach określonych w Procedurze.

Niniejszy formularz służy złożeniu w dobrej wierze zgłoszenia wewnętrznego o: uzasadnionym podejrzeniu wystąpienia naruszenia, rzeczywistym wystąpieniu naruszenia, istnieniu wysokiego ryzyka wystąpienia naruszenia lub prób ich ukrycia.

2. Osoba dokonująca zgłoszenia wewnętrznego:

Imię i nazwisko:

.....

Dane kontaktowe:

(proszę zaznaczyć odpowiednie okienko)

- jestem pracownikiem
- pracownikiem tymczasowym
- jestem zleceniobiorcą/usługodawcą
- świadczę pracę na innej podstawie niż stosunek pracy, w tym na podstawie innej umowy cywilnoprawnej
- przedsiębiorcą
- prokurentem
- jestem członkiem organu
- jestem byłym pracownikiem
- jestem kandydatem do pracy

- jestem wolontariuszem
- jestem praktykantem
- jestem stażystą
- świadcząc pracę pod nadzorem i kierownictwem wykonawcy/podwykonawcy/dostawcy, w tym na podstawie umowy cywilnoprawnej
- inne:

Stanowisko służbowe:
.....

3. Osoba, której naruszenia zgłoszenie wewnętrzne dotyczy

Imię i nazwisko:
.....

Stanowisko służbowe:
.....

4. Data i miejsce naruszenia oraz sposób, w jaki uzyskano wiedzę o naruszeniu

.....
.....
.....
.....
.....
.....
.....

5. Informacja czy podejmował/a Pan/Pani działania w celu eliminacji naruszenia, bądź ich skutków (np. wcześniejsze zgłoszenie sytuacji przełożonemu, poradzenie się itp.?)

.....
.....
.....
.....

.....
.....

6. Zwięzły opis naruszenia i przebieg zdarzenia ze wskazaniem istotnych faktów. Wskazanie rodzaju naruszenia, w tym jakie zostały naruszone przepisy prawa? Na czym polega naruszenie? W jaki sposób doszło do naruszenia? Z jakiego powodu wystąpiło naruszenie? W jaki sposób uzyskano o nim wiedzę? Jakie są skutki naruszenia?

.....
.....
.....
.....
.....
.....

7. Uwagi dodatkowe/Wszelkie inne dane i informacje

.....
.....
.....
.....
.....

8. Preferowana forma kontaktu – adres korespondencyjny, adres e-mail, numer telefonu itp., jeżeli dotyczy

.....
.....
.....

(podpis osoby składającej zgłoszenie wewnętrzne)

.....

(podpis osoby odpowiedzialnej za przyjęcie zgłoszenia wewnętrznego)

KLAUZULA INFORMACYJNA DLA SYGNALISTY (OSOBY SKŁADAJĄCEJ ZGŁOSZENIE WEWNĘTRZNE)

Administrator danych osobowych:	Poznański Ośrodek Specjalistycznych Usług Medycznych, 61-695 Poznań, Al. Solidarności 36, e-mail: sekretariat@posum.pl, nr tel. 61 647 77 77
Osoba odpowiedzialna za ochronę danych:	iod@posum.pl
Cel przetwarzania Obsługa zgłoszenia sygnalisty	Podstawa prawna przetwarzania Przetwarzanie odbywa się w celu wypełnienia obowiązku prawnego ciążącego na Administratorze polegającego na realizacji zadań związanych z obsługą zgłoszeń wewnętrznych na podstawie art. 6 ust. 1 lit. c) RODO w związku z ustawą z dnia 14 czerwca 2024 r. o ochronie sygnalistów (Dz.U.2024 poz. 928). Dane szczególnej kategorii, jeśli zostaną wskazane w zgłoszeniu Sygnalisty, będą przetwarzane na podstawie art. 9 ust. 2 lit. g) RODO w związku z przepisami ustawy o ochronie sygnalistów. Przez okres trwania rekrutacji.
Okres przetwarzania danych	Pani/Pana dane osobowe będą przechowywane przez okres 3 lat po zakończeniu roku kalendarzowego, w którym zakończono działania następcze, lub po zakończeniu postępowań zainicjowanych tymi działaniami.
Odbiorcy danych:	Dane mogą zostać: <ul style="list-style-type: none"> • powierzone partnerom technologicznym, czyli podmiotom świadczącym usługi takie jak hosting, wysyłka e-maili oraz świadczącym usługi statystyczne, obsługę portali społecznościowych oraz usługi rozwoju i utrzymania oprogramowania; • udostępnione organom prawa i administracji publicznej w przypadkach prawnie uzasadnionych.
Prawa związane z przetwarzaniem danych osobowych:	
Jeżeli podstawą prawną jest art. 6 ust. 1 lit. c) RODO:	Prawo dostępu do treści danych, prawo do sprostowania danych, prawo do ograniczenia przetwarzania danych.
Prawo wniesienia skargi do organu nadzorczego:	W przypadku stwierdzenia naruszeń ze strony Administratora, co do bezpieczeństwa przetwarzania tych danych, istnieje możliwość wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych.
Wymóg podania danych:	Podanie danych osobowych jest niezbędne do przyjęcia i rozpatrzenia zgłoszenia.
Automatyczne podejmowanie decyzji w tym profilowanie:	Nie dotyczy.

Załącznik nr 2 do Procedury – Wzór potwierdzenia otrzymania zgłoszenia wewnętrznego

.....
(miejsowość, data)

POTWIERDZENIE OTRZYMANIA ZGŁOSZENIA WEWNĘTRZNEGO

Niniejszym potwierdza się przyjęcie zgłoszenia wewnętrznego dotyczącego naruszenia, które zostało dokonane pisemnie (listownie/elektronicznie) przez

....., w dniu

polegającego na

..... mającego

miejsce w

.....

Pani/Pana dane osobowe oraz inne dane pozwalające na ustalenie Pani/Pana tożsamości nie podlegają ujawnieniu, chyba, że wyrazi Pani/Pan na to zgodę. Podane informacje objęte są poufnością w zakresie tożsamości osoby dokonującej zgłoszenia i osoby, której dotyczy zgłoszenie.

Informacja zwrotna w zakresie planowanych lub podjętych działań następczych w związku ze zgłoszeniem wewnętrznym naruszenia wraz z podaniem powodów takich działań, nastąpi w terminie nieprzekraczającym 3 miesięcy od potwierdzenia przyjęcia zgłoszenia, to jest do dnia (w przypadku nieprzekazania potwierdzenia sygnaliście, termin przekazania informacji zwrotnej wynosi 3 miesiące od upływu 7 dni od dnia dokonania zgłoszenia wewnętrznego) na adres do korespondencji/adres mailowy podany w zgłoszeniu naruszenia wewnętrznego.

.....

(podpis osoby odpowiedzialnej za przyjęcie zgłoszenia wewnętrznego)

Załącznik nr 3 do Procedury – Wzór rejestru zgłoszonych naruszeń

REJESTR ZGŁOSZEŃ WEWNĘTRZNYCH

Nr zgłoszenia	Przedmiot naruszenia	Dane osobowe sygnalisty niezbędne do identyfikacji sygnalisty.	Dane osobowe osoby, której zgłoszenie dotyczy niezbędne do identyfikacji takiej osoby	Adres do kontaktu sygnalisty	Data dokonania zgłoszenia	Informacja o podjętych działaniach następczych	Data zakończenia sprawy

Załącznik nr 4 do Procedury – Wzór oświadczenia o zapoznaniu się z procedurą zgłaszania informacji o naruszeniach prawa i podejmowania działań następczych

.....
(miejsowość, data)

**OŚWIADCZENIE O ZAPOZNANIU SIĘ Z PROCEDURĄ ZGŁASZANIA INFORMACJI O
NARUSZENIACH PRAWA I PODEJMOWANIA DZIAŁAŃ NASTĘPCZYCH
OBOWIĄZUJĄCA
W POSUM**

Oświadczam, że zapoznałem się treścią wewnętrznej Procedury zgłaszania informacji o naruszeniach prawa i podejmowania działań następczych obowiązującą w POSUM w Poznaniu.

.....
(podpis osoby składającej oświadczenie)

Załącznik nr 5 do Procedury – Wzór klauzuli informacyjnej dla osób wskazanych w zgłoszeniu wewnętrznym

Administrator danych osobowych:	Poznański Ośrodek Specjalistycznych Usług Medycznych, 61-695 Poznań, Al. Solidarności 36, e-mail: sekretariat@posum.pl, nr tel. 61 647 77 77
Osoba odpowiedzialna za ochronę danych:	iod@posum.pl
Cel przetwarzania Obsługa zgłoszenia sygnalisty	Podstawa prawna przetwarzania Państwa dane osobowe będą przetwarzane w celu wypełnienia obowiązku prawnego ciążącego na Administratorze polegającego na realizacji zadań związanych z obsługą zgłoszeń wewnętrznych na podstawie art. 6 ust. 1 lit. c) RODO w związku z ustawą z dnia 14 czerwca 2024 r. o ochronie sygnalistów (Dz.U.2024 poz. 928). Dane szczególnej kategorii, jeśli zostaną wskazane w zgłoszeniu Sygnalisty, będą przetwarzane na podstawie art. 9 ust. 2 lit. g) RODO w związku z przepisami ustawy o ochronie sygnalistów.
Okres przetwarzania danych	Pani/Pana dane osobowe będą przechowywane przez okres 3 lat po zakończeniu roku kalendarzowego, w którym zakończono działania następcze, lub po zakończeniu postępowań zainicjowanych tymi działaniami.
Odbiorcy danych:	Dane mogą zostać: <ul style="list-style-type: none"> • powierzone partnerom technologicznym, czyli podmiotom świadczącym usługi takie jak hosting, wysyłka e-maili oraz świadczącym usługi statystyczne, obsługę portali społecznościowych oraz usługi rozwoju i utrzymania oprogramowania; • udostępnione organom prawa i administracji publicznej w przypadkach prawnie uzasadnionych.
Prawa związane z przetwarzaniem danych osobowych:	
Jeżeli podstawą prawną jest art. 6 ust. 1 lit. c) RODO:	Prawo dostępu do treści danych, prawo do sprostowania danych, prawo do ograniczenia przetwarzania danych.
Prawo wniesienia skargi do organu nadzorczego:	W przypadku stwierdzenia naruszeń ze strony Administratora, co do bezpieczeństwa przetwarzania tych danych, istnieje możliwość wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych.
Wymóg podania danych:	Administrator przetwarza dane osobowe wskazane w zgłoszeniu Sygnalisty (dane identyfikacyjne, takie jak imię i nazwisko). Dane te zostały przekazane przez Sygnalistę.
Automatyczne podejmowanie decyzji w tym profilowanie:	Nie dotyczy.

Załącznik nr 6 do Procedury – Wzór upoważnienia do przetwarzania danych osobowych

Poznań, dnia

UPOWAŻNIENIE **do przetwarzania danych osobowych w związku z wewnętrznymi zgłoszeniami** **naruszeń prawa**

Z dniem upoważniam Panią/Pana

.....

podać imię i nazwisko osoby upoważnionej

do przetwarzania danych osobowych Sygnalistów i innych osób w związku z realizacją procedury zgłoszeń wewnętrznych naruszeń prawa, w szczególności w ramach przyjmowania i weryfikacji zgłoszeń naruszeń prawa, podejmowania działań następczych, komunikacji z Sygnalistą i przekazywania mu informacji zwrotnej.

Jednocześnie, wraz z nadanym upoważnieniem, zobowiązuję Panią/Pana do przestrzegania przepisów dotyczących ochrony danych osobowych oraz wprowadzonych i wdrożonych do stosowania przez Administratora dokumentów wewnętrznym, w szczególności Polityki Bezpieczeństwa.

Niniejsze upoważnienie traci moc:

z dniem *(podać datę dla upoważnienia czasowego)* lub odwołania albo rozwiązania lub wygaśnięcia umowy o pracę, umowy zlecenia, umowy o dzieło lub innej umowy cywilnoprawnej łączącej Pana/Panią z Administratorem.

.....

.....

Miejscowość, data

podpis Administratora

OŚWIADCZENIE

Oświadczam, iż zostałam/em zapoznana/y z przepisami dotyczącymi ochrony danych osobowych, w szczególności Rozporządzenia Parlamentu Europejskiego i Rady UE z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) Tekst mający znaczenie dla EOG, wydanych na jej podstawie aktów wykonawczych oraz wprowadzonych i wdrożonych do stosowania przez Administratora Polityki Bezpieczeństwa Danych.

Zobowiązuję się do:

- zachowania w tajemnicy danych osobowych jak również innych informacji stanowiących tajemnicę przedsiębiorcy w rozumieniu ustawy z dnia 16 kwietnia 1993r. o zwalczaniu nieuczciwej konkurencji (tekst jednolity Dz. U. z 2018 r. poz. 419 z późn. zm.) do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań służbowych lub obowiązków pracowniczych,
- niewykorzystywania danych osobowych oraz innych informacji w celach pozasłużbowych o ile nie są one jawne,
- zachowania w tajemnicy sposobów zabezpieczenia danych osobowych oraz innych informacji o ile nie są one jawne,
- korzystania ze sprzętu IT oraz oprogramowania wyłącznie w związku z wykonywaniem obowiązków,
- wykorzystywania jedynie legalnego oprogramowania pochodzącego od Administratora,
- należytej dbałości o sprzęt i oprogramowanie zgodnie z dokumentacją przetwarzania danych osobowych,
- korzystania z komputerów przenośnych zgodnie z dokumentacją przetwarzania danych osobowych,
- nieudostępniania sprzętu służbowego, w szczególności urządzeń mobilnych, osobom trzecim.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami, może być uznane przez POSUM za ciężkie naruszenie obowiązków pracowniczych w rozumieniu art. 52 § 1 pkt 1 Kodeksu Pracy lub za naruszenie przepisów karnych ww. ustawy o ochronie danych osobowych lub ciężkie naruszenie obowiązków umownych w przypadku umowy cywilnoprawnej.

.....
.....
podpis osoby upoważnionej

Załącznik nr 7 do Procedury – Pomocnicza instrukcja szyfrowania zawartości przesyłki (zgłoszenia dokonywane elektronicznie)

Pomocnicza instrukcja szyfrowania zawartości przesyłki ze zgłoszeniem wewnętrznym pisemnym, dokonywanym na adres: zgloszenie.wewnetrzne@posum.pl

1. Hasło do otwarcia zaszyfrowanych plików - powinno charakteryzować się odpowiednią złożonością stanowiącą kombinację wielkich i małych liter, cyfr i symboli
2. Szyfrowanie plików - ZIP

- Wysłasz mailem plik zawierający **dane prawnie chronione**, w tym dane osobowe do klienta, a może do współpracownika?
- Potrzebujesz przenieść plik zawierający dane z jednego komputera na drugi używając **pendriva**?

Pamiętaj, aby zadbać
o bezpieczeństwo danych poprzez

ZASZYFROWANIE PLIKÓW

To Twój zabezpieczony folder, który możesz bezpiecznie wysłać/przenieść!

Jeśli wysyłasz / przenosisz plik pamiętaj, by przekazać **hasło** drugiej osobie innym kanałem:
smsem lub telefonicznie.

3. Szyfrowanie plików - Win RAR

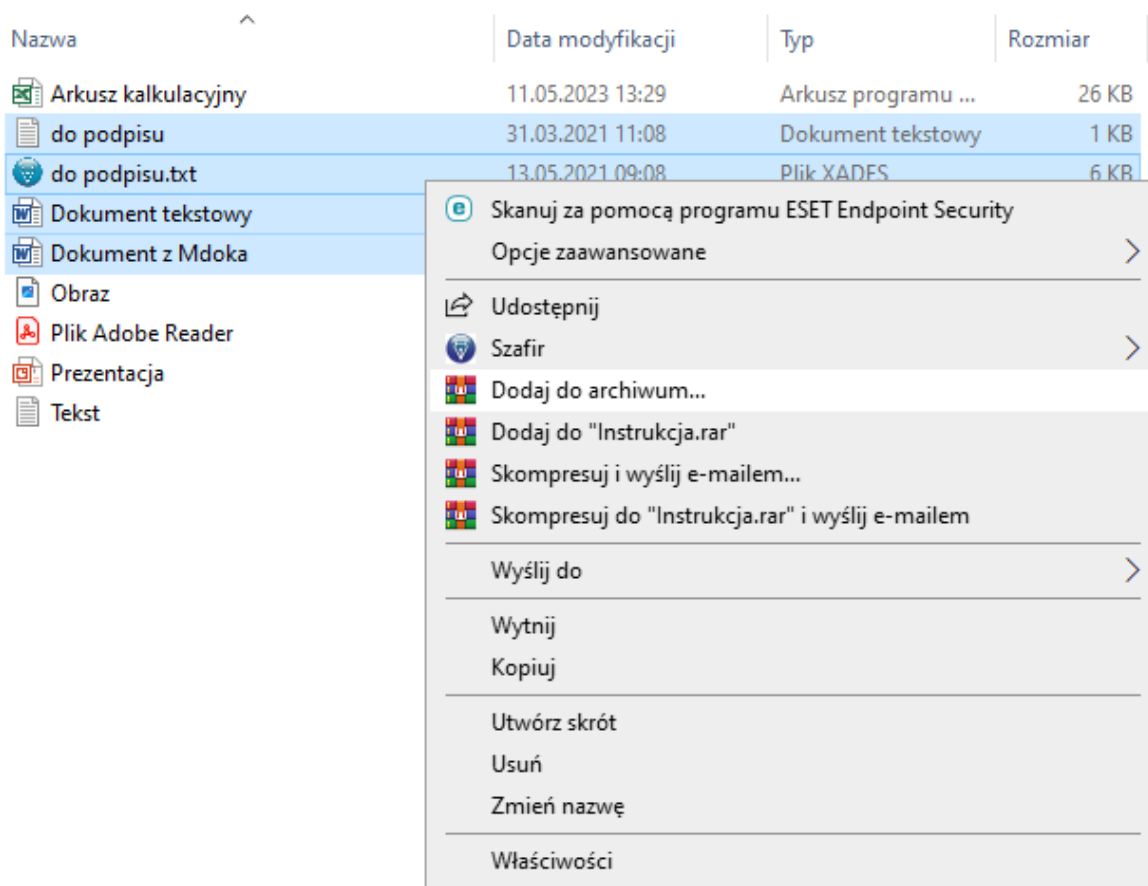
- Niniejsza instrukcja przeznaczona jest dla pracowników UMP i przedstawia metodę szyfrowania plików elektronicznych. Obejmuje skrócony opis obsługi programu WinRAR w wersji 6.x z wykorzystaniem zabezpieczenia kryptograficznego.

Kompresowanie plików

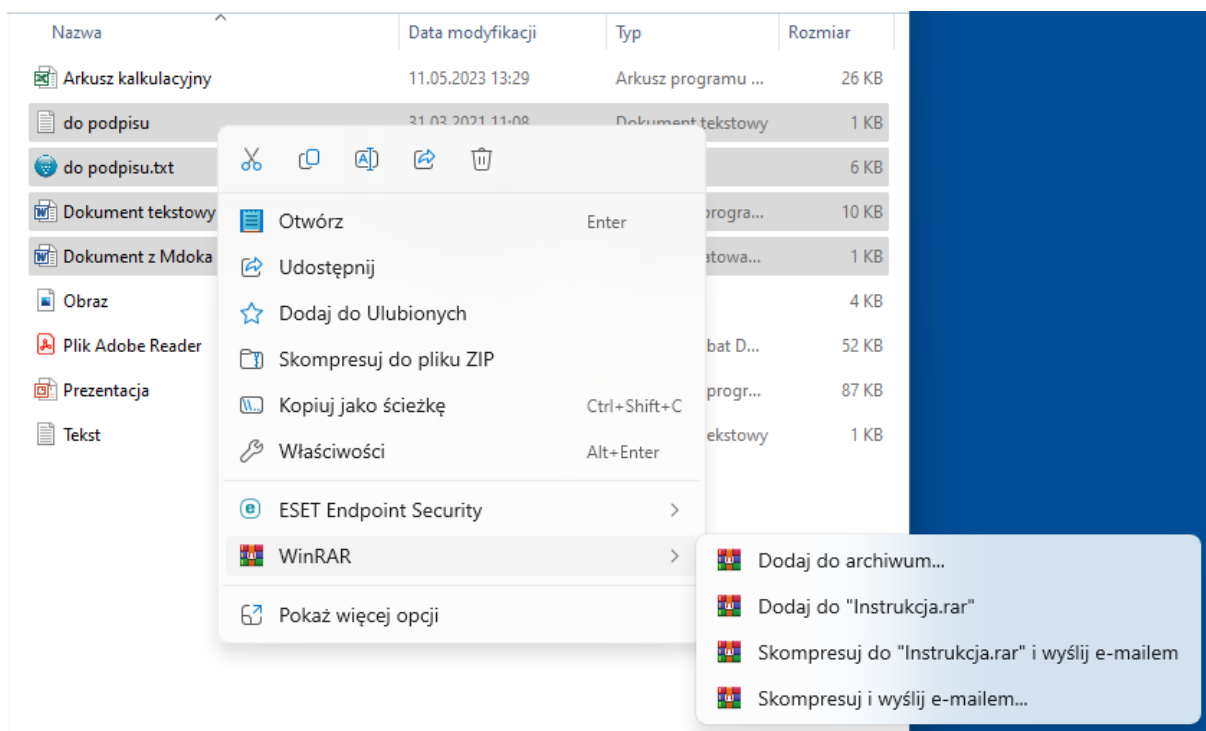
- Przed przystąpieniem do utworzenia zaszyfrowanego archiwum proponowane jest umieszczenie wszystkich plików, które mają stanowić archiwum w nowym folderze.

Zaznacz pliki i wywołaj WinRAR

- W oknie eksploratora Windows zaznacz pliki, które będą podlegały archiwizacji i kliknij na nich prawym klawiszem myszki.
- Z menu kontekstowego wybieramy „Dodaj do archiwum...”



WIDOK MENU KONTEKSTOWEGO - WINDOWS 10



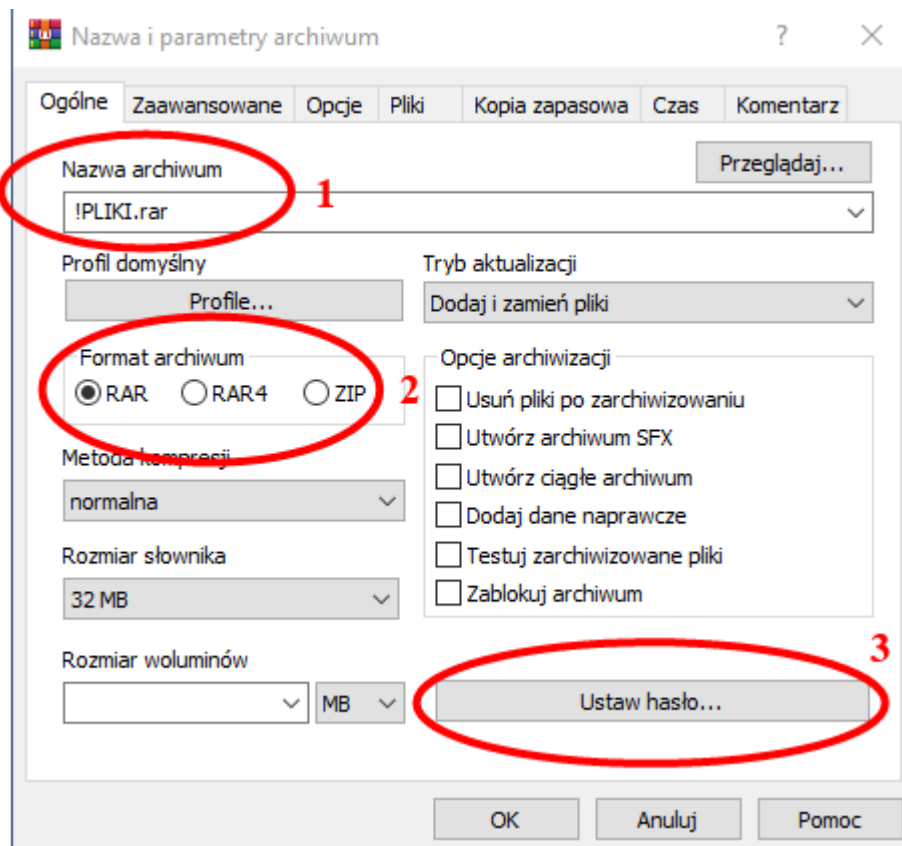
WIDOK MENU KONTEKSTOWEGO - WINDOWS 11

Ustaw parametry:

1. Nazwa archiwum (nazwa jest podawana domyślnie, użytkownik może ją zmienić, nie jest wymagane rozszerzenie .rar).
2. Format archiwum (domyślnie podpowiadane RAR).

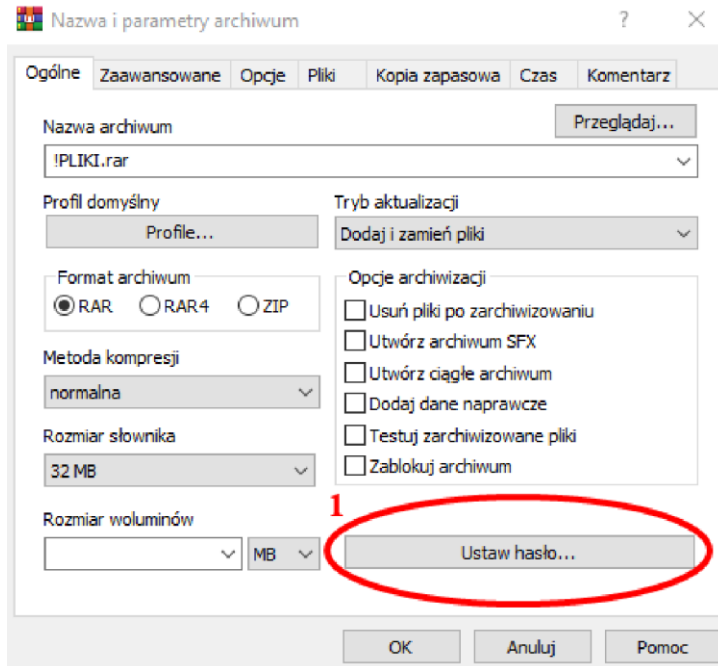
UWAGA – W przypadku tworzonego archiwum służącego do realizacji zadań publicznych zgodnie z Rozporządzeniem Rady Ministrów z dnia 24-05-2024 r. w sprawie Krajowych Ram Interoperacyjności zaleca się zaznaczanie formatu ZIP.

3. Wprowadzanie hasła w celu zabezpieczenia kryptograficznego pliku archiwum.

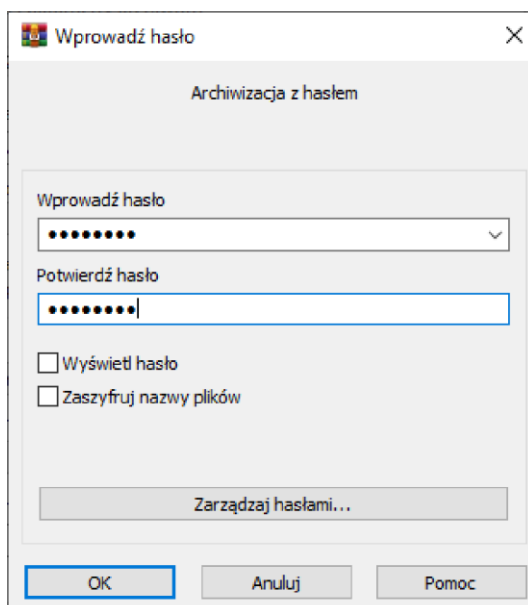


Wprowadzanie hasła

Kliknij na przycisk 1 „Ustaw hasło...” w celu zabezpieczenia kryptograficznego pliku archiwum.



Wprowadź i potwierdź hasło, a następnie naciśnij OK.

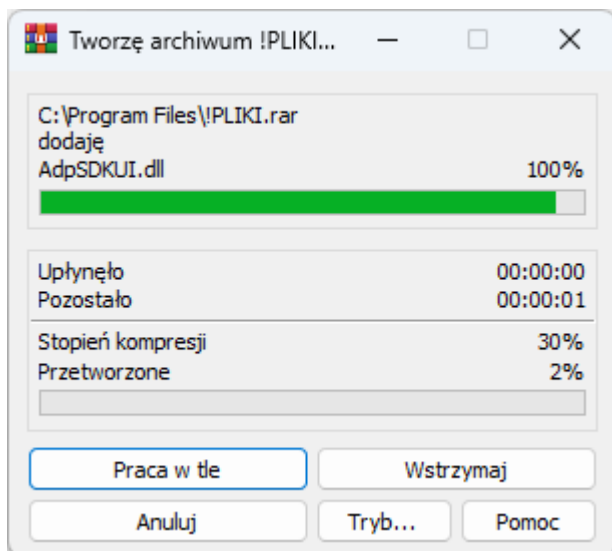


Zakończenie

Po zdefiniowaniu parametrów (opisanych powyżej), czasowo pojawi się okno przedstawiające paski postępu przygotowania archiwum.

Wynikiem jest plik szyfrowanego archiwum o rozszerzeniu *.RAR lub *.ZIP.

Otwarcie pliku wymaga podania wprowadzonego hasła.



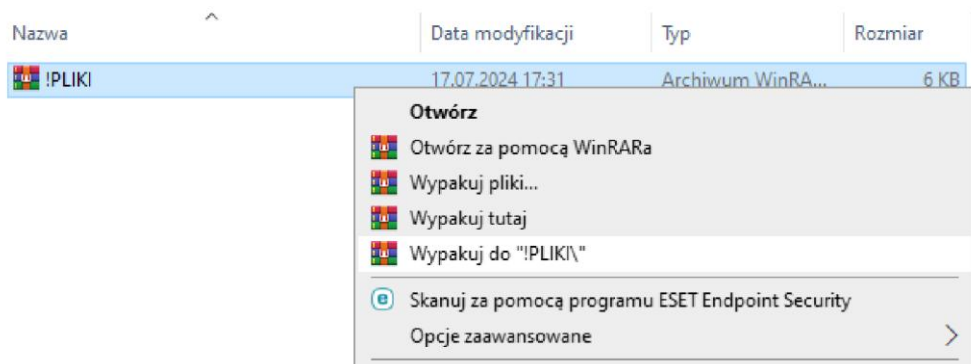
Wyodrębnianie plików

Przed przystąpieniem do odczytania lub wypakowania zaszyfrowanego archiwum proponowane jest umieszczenie go w nowym folderze.

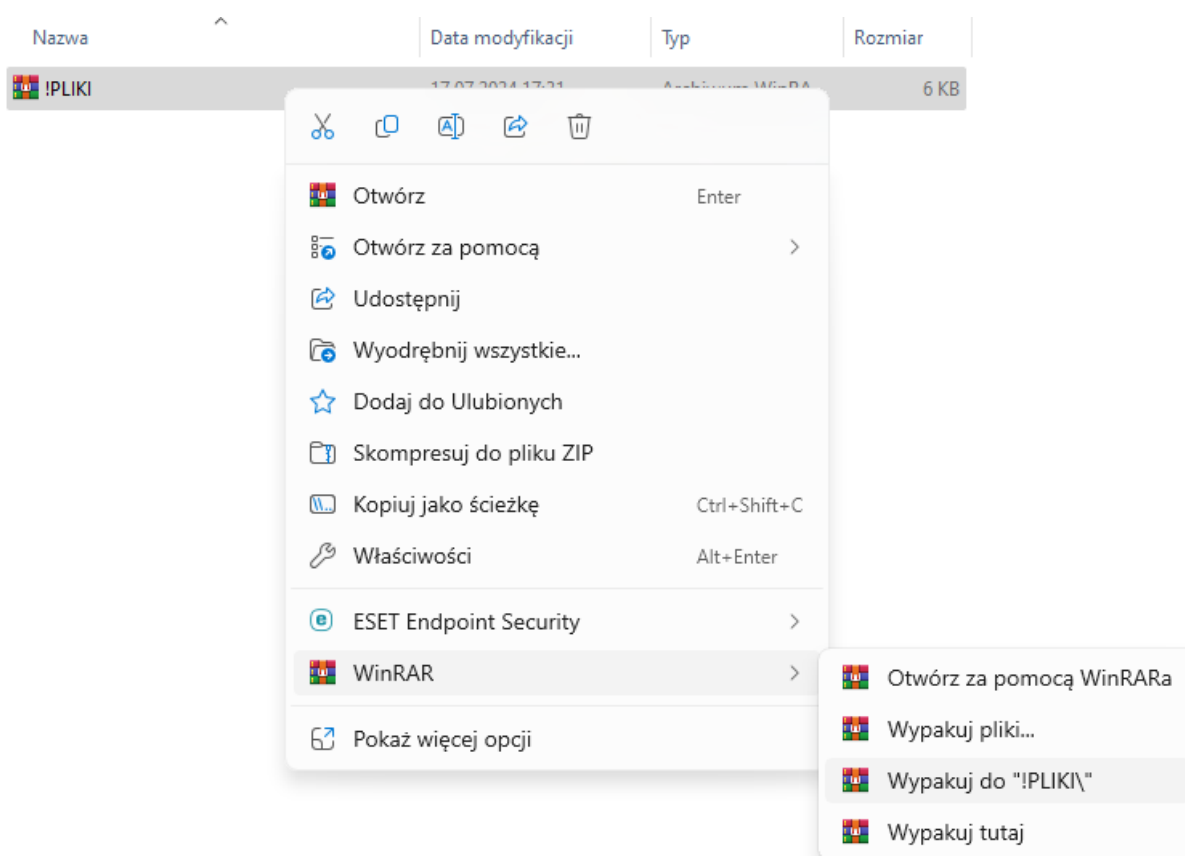
Wywołaj program WinRAR

W oknie eksploratora Windows zaznacz plik archiwum i kliknij na nim prawym klawiszem myszki.

Z menu kontekstowego wybieramy „Wypakuj do !PLIKI” Nazwa !PLIKI jest zmienna i uzależniona od nazwy posiadanego pliku archiwum.



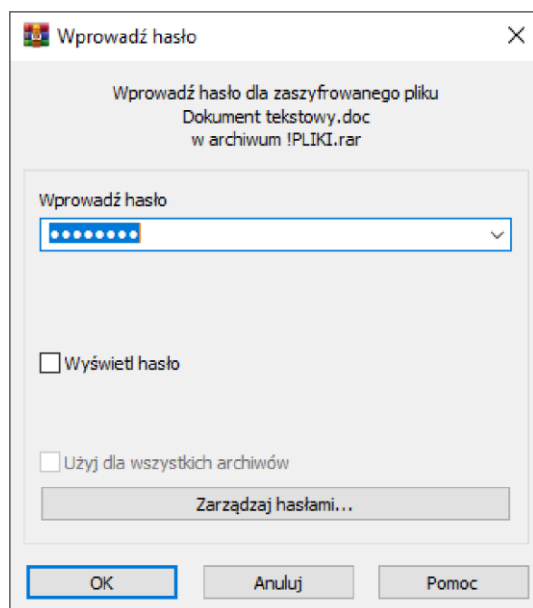
WIDOK MENU KONTEKSTOWEGO - WINDOWS 10



WIDOK MENU KONTEKSTOWEGO - WINDOWS 11

Wprowadź hasło

W przypadku zaszyfrowanego archiwum pojawi się okno z prośbą o podanie odpowiedniego hasła. Wprowadź hasło i naciśnij OK.



Umieszczenie plików

Prawidłowe rozpakowanie archiwum umieszcza pliki w folderze będącym nazwą archiwum

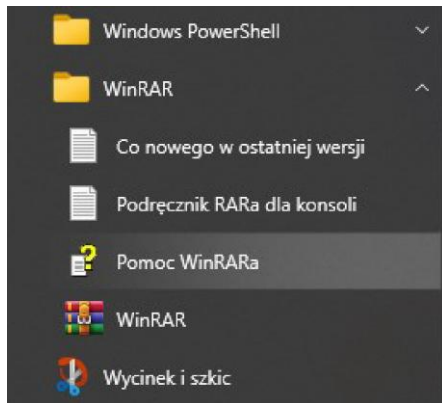
w naszej instrukcji jest to folder **!PLIKI**.

Nazwa	Data modyfikacji	Typ	Rozmiar
!PLIKI	17.07.2024 17:54	Folder plików	
!PLIKI	17.07.2024 17:45	Archiwum WinRA...	6 KB

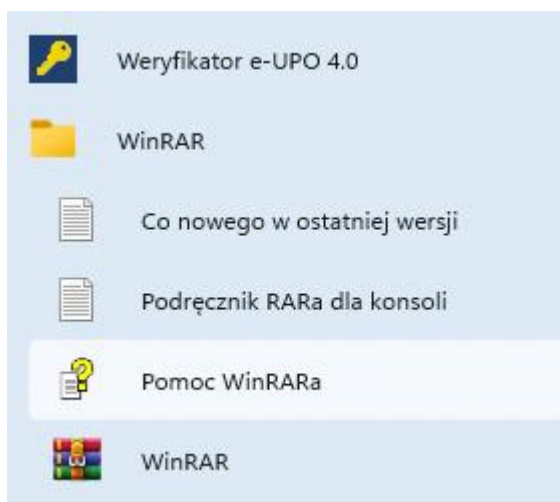
Uwagi końcowe

Niniejsza instrukcja przedstawia jeden ze sposobów kompresji plików wraz z ich szyfrowaniem.

Pełne informacje na temat programu WinRAR można znaleźć w obszernej instrukcji załączonej przy instalacji: *Pomoc WinRARa*.



WIDOK - WINDOWS 10



WIDOK - WINDOWS 11